# Article information:

KCC Method: Unknown Intrusion Detection Based on Open Set Recognition | IEEE Conference Publication | IEEE Xplore
<https://ieeexplore.ieee.org/document/9643172>

# Article summary:

1. The KCC (Known Central Clustering) method is proposed to improve the ability of deep learning tools to deal with intrusion detection problems based on open set recognition.

2. The KCC method introduces CD-loss (Class Distance-loss) to get the centers of different class clusters and negative samples as the unknown classes for training to obtain the threshold of the known classes.

3. Experiments on CIC-IDS2017 and CIC-DDoS2019 datasets show that the KCC method improves the classification accuracy of known intrusions and reduces the misclassification rate of unknown intrusions.

# Article rating:

May be slightly imbalanced: The article presents the information in a generally reliable way, but there are minor points of consideration that could be explored further or claims that are not fully backed by appropriate evidence. Some perspectives may also be omitted, and you are encouraged to use the research topics section to explore the topic further.

# Article analysis:

The article provides a detailed overview of an intrusion detection system based on open set recognition, which uses deep learning tools to distinguish between normal traffic and intrusions. The article is well written and provides a comprehensive description of the proposed KCC (Known Central Clustering) method, its components, and how it works in practice. The authors also provide evidence from experiments conducted on two datasets, showing that their proposed method improves classification accuracy for known intrusions and reduces misclassification rate for unknown intrusions.

The article appears to be reliable and trustworthy overall, as it provides a clear explanation of its methods and results, as well as evidence from experiments conducted on two datasets. However, there are some potential biases in the article that should be noted. For example, while the authors do mention existing methods such as OpenMax, they do not provide any comparison between their proposed method and these existing methods in terms of performance or accuracy. Additionally, while they do mention possible risks associated with their proposed system, they do not provide any details about how these risks can be mitigated or avoided. Furthermore, while they discuss applications in computer vision related to open set recognition algorithms, they do not explore any counterarguments or other potential applications outside this field.

In conclusion, this article is generally reliable and trustworthy overall but there are some potential biases that should be noted when considering its content.

# Topics for further research:

* Open set recognition algorithms
* Comparison of intrusion detection systems
* Mitigation of risks associated with intrusion detection systems
* Applications of open set recognition algorithms
* Performance evaluation of intrusion detection systems
* Counterarguments to open set recognition algorithms

# Report location:

<https://www.fullpicture.app/item/71531000d2dde20bbab8075bf58a1e32>